

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MICHAEL GORDON DOUGLAS,

Defendant.

Case No.: 23-CR-80219-AMC

**NOTICE OF UNITED STATES' INTENT TO
OFFER EVIDENCE UNDER RULES 702, 703,
AND 705 & REQUEST FOR RECIPROCAL
DISCOVERY**

PLEASE TAKE NOTICE that Plaintiff, UNITED STATES OF AMERICA, intends to offer evidence under Rules 702, 703, and 705 of the Federal Rules of Evidence in its case-in-chief at trial in this case.

1. Notice of Evidence Under Rules 702, 703, and 705

Pursuant to Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure and Southern District of Florida Local Rule 88.10(o)(3)(A), the United States provides the following disclosure concerning the potential expert testimony of Computer Forensic Agent Scott J. Unger of the Department of Homeland Security, Homeland Security Investigations ("HSI") that the United States may seek to introduce at trial pursuant to Rules 702, 703, and 705 of the Federal Rules of Evidence. The United States also reserves the right to offer additional testimony by this expert, or other expert witnesses, and for the experts to amend or adjust their opinions and bases therefor, based on information perceived by or made known to the experts before or during trial.

Agent Unger has worked as a Computer Forensic Agent with HSI since 2021. In this position, he conducts computer forensic extractions and analysis. In particular, he regularly conducts and assists other investigators with conducting forensic analysis of seized computer

systems, mobile devices, and other digital media to provide investigative and analytical support to prosecutors and law enforcement agents. He has conducted and assisted with numerous investigations of offenses involving the online sexual exploitation of children, and regularly assists other HSI investigators with the onsite seizure and examination of digital evidence pursuant to federal search warrants. Prior to his current position, Agent Unger worked as a special agent in Ft. Lauderdale and Miami from 2011 through 2021.

Agent Unger has numerous certifications, including from Homeland Security Investigations as Computer Forensic Agent, from GetData Forensics as a Forensic Explorer Certified Examiner and from CompTIA in CompTIA A+. In addition to his on-the-job experience analyzing digital devices, he has taken numerous training courses connected to the analysis of computers, mobile devices, and other digital evidence. He also holds a bachelor's degree in criminal justice from Florida Atlantic University in Boca Raton, Florida. A copy of Agent Unger's curriculum vitae will be produced in discovery.

In the last four years, Agent Unger has not testified as an expert witness. Agent Unger has also not authored any publications in the last ten years.

The Extraction of Data from Digital Devices

Although the United States does not believe that testimony regarding the extraction of data from digital devices is expert testimony under the Federal Rules of Evidence,¹ in an abundance of caution the United States is providing notice that, absent a signed stipulation between the parties,

¹ See *United States v. McLeod*, 755 Fed. Appx. 670, 673-74 (9th Cir. 2019) (unpublished) (district court did not abuse its discretion by admitting testimony without requiring compliance with Rule 702 where witness testified about what Cellebrite does, how he used it to extract information from a cell phone, and how he could select what data to extract); *United States v. Seugasala*, 702 F. App'x 572, 575 (9th Cir. 2017) (unpublished) ("The officers who followed the software prompts from Cellebrite and XRY to obtain data from electronic devices did not present testimony that was based on technical or specialized knowledge that would require expert testimony.")

it intends to offer testimony from Agent Unger regarding the process through which he uses forensic tools to extract and analyze data from seized digital devices.

The defendant is charged with distribution of child pornography and attempted enticement of a minor. As part of his investigation in the above-captioned case, Agent Unger examined multiple digital devices including cellular phones, computer devices, and online storage accounts. These devices and accounts were seized from the defendant's residence and vehicle, and seized from third-party service providers pursuant to federally issued search warrants.

In particular, after testifying about his training and background discussed above, Agent Unger may testify about: the physical inventorying of a digital device, such as a phone and other devices and online accounts, once it is identified during the execution of a warrant and then submitted as an evidence item in an investigation. He will explain the extraction of material from such devices and accounts into programs that allow for searching and viewing in an easier manner than reviewing the original content; and the reliability of the various programs that he uses to parse, examine, and analyze the matching data contained on the forensic image copy of the digital evidence item.

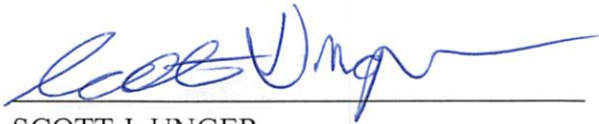
Agent Unger is likewise expected to testify as to how, with respect to the devices that HSI seized in the above-captioned case.

The Forensic Examination of Digital Devices

In addition to testifying that reliable forensic tools were used to extract, parse, and examine data from the defendants' digital devices, Agent Unger is also expected to testify about the results of the forensic examination of these devices. In this sense, Agent Unger will be testifying more in the nature of a fact witness, explaining how he was able to locate and preserve certain evidence from the forensic image copies of the devices he examined. Nevertheless, out of an abundance of

caution, the United States is also providing notice that it intends to offer testimony from Agent Unger regarding the results of the forensic examinations of the seized devices referenced above.

The results of the forensic examination of these digital devices and online storage accounts have been made available to the defense for their review at the HSI offices in West Palm Beach or by their own digital forensic examiner at the HSI offices in West Palm Beach.² Accordingly, pursuant to Fed. R. Crim. P. 16(a)(1)(F) & (G)(iv), the results of the forensic examination of these devices will not be repeated in full here. Generally speaking, however, Agent Unger may testify as to how the above devices and accounts contained child pornography, chat communication, distribution of child pornography, internet searches related to child exploitation, and evidence tying the use and ownership of a particular device to the defendant.



SCOTT J. UNGER
Computer Forensic Agent, Homeland Security Investigations

² Consistent with 18 U.S.C. § 3509(m), the United States has made and will continue to make the contraband evidence recovered through the forensic examination of these devices reasonably available to the defense at an appropriate government facility.

2. Notice of Request for Reciprocal Discovery

With respect to the defendant in this matter, the United States requests the following.

Under Rule 16(b)(1)(A), the United States requests to inspect, copy, and photograph any and all books, papers, documents, photographs, tangible objects, or make copies of portions thereof, which are within the possession, custody or control of the defendant and that the defendant intends to introduce as evidence in his case-in-chief at trial.

Under Rule 16(b)(1)(B), the United States requests to inspect and copy or photograph any results or reports of physical or mental examinations and of scientific tests or experiments made in connection with this case, which are in the possession or control of the defendant that he intends to introduce as evidence at the trial or that were prepared by a witness whom the defendant intends to call.

Under Rule 16(b)(1)(C), the United States requests a written statement of any testimony that the defendant intends to use under Rules 702, 703, and/or 705 of the Federal Rules of Evidence as evidence at trial. This statement must include a complete statement of all opinions that the defendant will elicit from the witness in the defendant's case-in-chief; the bases and reasons for them; the witness's qualifications, including a list of all publications authored in the previous 10 years; and, a list of all other cases in which, during the previous 4 years, the witness has testified as an expert at trial or by deposition.

The United States also asks for prior statements of all witnesses (except the defendant) under Rule 26.2.

MARKENZY LAPOINTE
UNITED STATES ATTORNEY

By: s/Gregory Schiller
Gregory Schiller
Assistant United States Attorney
Florida Bar No. 0648477
500 S. Australian Ave., Suite 400
West Palm Beach, FL 33401
Tel: (561) 209-1045
Email: gregory.schiller@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on July 18, 2024, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF.

s/Gregory Schiller
Gregory Schiller
Assistant United States Attorney